Cyberwarfare o Ciberguerra

RAFAEL QUIÑONES

El ensayo nos introduce en un tema que ha estado, en los últimos años, en el tapete de la dicusión política: el ciberespionaje. Empieza por aclararnos el término visto a través de diversos autores y las consecuencias del mismo. Nos habla de sus motivaciones y de los beneficios políticos y económicos. Igualmente nos ofrece algunos ejemplos de esa actividad.

INTRODUCCIÓN

Podemos definir de forma genérica y sencilla el término ciberespionaje como todo acto de una información, de individuos, competidores, rivales, grupos, gobiernos y especialmente enemigos, para obtener de eso alguna ventaja, sea personal, económica, política o militar, utilizando los recursos tecnológicos de Internet, computadoras personales y redes, a través del uso de técnicas de *cracking* y *software* maliciosos incluyendo troyanos y *spyware* (Encyclopedia Indes: A-Z/ PCMag). De esta forma, dicho acto puede concretarse completamente desde las computadoras personales de expertos en dichas actividades, ya sean amateurs desde sus hogares, o espías gubernamentales entrenados para esas lides.

El ciberespionaje, por lo general, implica el acceso a los secretos y archivos clasificados o el control de ordenadores individuales o redes enteras para una estrategia avanzada. En los tiempos recientes se ha descubierto que el ciberespionaje supone también el análisis de la actividad pública en redes sociales como Facebook y Twitter tanto de individuos como de grupos, organizaciones y demás colectivos.

Las motivaciones del ciberespionaje provienen de posibles beneficios políticos y económicos considerando que puede ser difícil de rastrear. Tales actividades, no como el espionaje cibernético típico, son ilegales en el país de la víctima mientras que son apoyadas totalmente por el más alto nivel de gobierno en el país del atacante. La situación ética igualmente depende del punto de vista de uno mismo, particularmente de la opinión de los gobiernos involucrados en el uso de estos métodos. Luego de esta breve introducción de las nociones sobre lo que trata el ciberespionaje, pasemos a los elementos en que dicha actividad está tocando o afectando elementos medulares de las sociedades humanas.

EL GRAN HERMANO SIEMPRE OBSERVA

George Orwell, en su inolvidable novela distópica *1984*, nos habló de un Estado totalitario todopoderoso que podía saber cualquier cosa de

su población a través del espionaje. Uno de los elementos tecnológicos que más recordará el lector de la novela es la telepantalla, un precusor del televisor que tenía la capacidad no solo de emitir información como una televisión, sino de forma bidireccional vigilar en todo momento el hogar y los habitantes donde dicho aparato estaba instalado y transmitiendo. En resumidas cuentas, la vigilancia permanente de los habitantes de un país por parte de su propio gobierno. Ahora, en la tercera década del siglo XXI no existen telepantallas para espiar a los ciudadanos, pero sí otras tecnologías vinculadas a la Internet y las computadoras personales que cumplen esa función. Igualmente, estas prácticas no son exclusivas de gobiernos totalitarios, ni siquiera de los autoritarios, sino de buena parte de los países democráticos de los que llamamos Occidente.

[...] cuando se comete un delito y un individuo es uno de los sospechosos enumerados, sus declaraciones hechas en las redes sociales pueden usarse en su contra en un tribunal de justicia. No solo eso, sino que también se puede utilizar lo que busca, descarga y a lo que accede en Internet.

Ryan Matthew Pierson, en noviembre de 2011, publicó un sustancioso artículo de opinión llamado "Cinco formas en que el gobierno te espía". El autor comienza su escrito afirmando que el Estado –aún en democracia– (en su caso, Estados Unidos) rastrea las actividades y el paradero de la gente promedio en nombre de la seguridad. Matthew Pierson recalca que dichos métodos a menudo se dan por sentados, aunque es importante comprender por parte de la ciudadanía en democracia exactamente qué parte de su vida pública y privada está siendo rastreada intencionalmente por una organización pagada con los dólares de los impuestos de los ciudadanos.

El autor argumenta que es fácil para el ciudadano promedio obviar el avance gradual de políticas y procedimientos que se imponen en nuestra vida privada porque vienen uno por uno durante un largo período de tiempo, especialmente desde la masificación del Internet en las sociedades contemporáneas. Matthew Pierson enumera cinco formas en que un gobierno puede espiar a sus ciudadanos.

1. Teléfonos móviles: en el caso de Estados Unidos (USA), la policía tiene dispositivos de extracción de datos fabricados por una empresa llamada Cellebrite (el caso pionero, la policía de Michigan). Dichos dispositivos se conectan directamente a las conexiones de datos de la mayoría de los teléfonos móviles y pueden descargar fotos, mensajes de texto, correo electrónico e incluso datos de GPS. El motivo por el que los agentes necesitan esta información puede requerir más investigación y no se requiere una orden judicial para el uso de estos extractores de datos de dispositivos móviles. En el 2010, Apple y Google fueron criticados por las funciones integradas dentro de sus móviles que rastreaban las coordenadas GPS de un teléfono e informaban esta ubicación a las oficinas centrales de Apple y Google. Apple abordó rápidamente esta controversia, lo que resultó en actualizaciones del *firmware* del iPhone que limita la cantidad de seguimiento que se realiza en el dispositivo. Según un estudio de Ars Technica, quedó en evidencia el período de tiempo en el que varios proveedores de servicios inalámbricos almacenan sus datos de uso. Según su estudio, los clientes de AT&T están sujetos a un almacenamiento de datos que dura entre tres y siete años, según el tipo de información involucrada. El contenido de los mensajes de texto de los clientes de Verizon se almacena de tres a cinco días y la información de la sesión de IP durante un año. Esta información, tal como existe, se puede citar o acceder a ella a través de una orden judicial en caso de que el investigado sea objeto de una investigación por parte de su agencia de aplicación de la ley local, estatal o federal.
2. Vigilancia pública general: todos conocemos la tecnología de cámaras en lugares públicos en muchas partes del mundo, especialmente en Estados Unidos. Pero Pierson señala la existencia de una tecnología llamada Intellistreets, que posibilita a dichas cámaras tomar

fotografías de las personas que pasan y escuchar conversaciones cercanas.

3. Pre-crimen: como su nombre lo indica, inspirado en el relato corto de ciencia ficción de Philip K. Dick, "Minority report", las agencias federales de seguridad en USA disponen de tecnologías que detectan cambios en el movimiento, el habla, la respiración, la frecuencia de parpadeo, las alteraciones del calor corporal y otros signos reveladores de que alguien está mintiendo o escondiendo algo activamente. Se ha dicho que estas tecnologías podrían llegar a los aeropuertos y otros lugares públicos que se cree son propensos a ataques terroristas u otros delitos violentos.

4. Medios de comunicación social: según Matthew Pierson, el Departamento de Seguridad –para el año en que escribió su artículo– está revisando activamente los sitios de redes sociales, incluidos Twitter y Facebook. En 2010, se reveló que a los agentes federales se les incentivó a detectar a amigos de personas en las redes sociales con el fin de brindar información para la oficina de Detección de Fraudes y Seguridad Nacional. Según el escritor, esto no era ninguna sorpresa, considerando la cantidad de información que la gente comparte fácilmente en las redes sociales: cuando se comete un delito y un individuo es uno de los sospechosos enumerados, sus declaraciones hechas en las redes sociales pueden usarse en su contra en un tribunal de justicia. No solo eso, sino que también se puede utilizar lo que busca, descarga y a lo que accede en Internet.

5. Actividad web: tanto a través del periodismo como de la ficción policiaca, hemos visto informes que revelan que un presunto asesino buscó términos para acceder a métodos para matar a alguien. El FBI y otras agencias han presionado a los principales ISP para que almacenen información sobre sus usuarios durante un período de al menos dos años.

Si en Estados Unidos, como cuna de la democracia moderna, estas actividades de ciberespionaje son frecuentemente practicadas sobre su ciudadanía, es obvio deducir que en regímenes autoritarios, dichas prácticas no solo se replican, sino que también son aún más intrusivas.

LOS BUENOS APRENDEN, PERO LO MALOS TAMBIÉN

Fabio Almada Torres, en junio de 2020, escribió un esclarecedor artículo llamado "Dictaduras digitales: cuando la tecnología refuerza la autocracia", que explica muchos detalles de las nuevas tecnologías de ciberespionaje a favor de las autocracias actuales del mundo. El autor comienza su escrito recordándonos la inmensa eficacia del Ministerio para la Seguridad del Estado de la República Democrática de Alemania, mejor conocida como STASI. Esta policía secreta consiguió crear una red que intervenía teléfonos, se infiltraba en movimientos políticos y reportaba relaciones personales y familiares de los ciudadanos del país comunista. Si bien el comunismo cayó en casi todo el mundo, las nuevas tecnologías permiten a las dictaduras contemporáneas nuevas formas de espiar de forma permanente a los habitantes del país en que gobiernan, a la altura de la extinta STASI.

Almada Torres señala que existe un método de vigilancia impulsada por algoritmos de "deep learning" e inteligencia artificial, y han demostrado que es posible automatizar y mejorar las tácticas de la STASI a un nivel mucho menos intrusivo, en el cual se necesitan menos recursos humanos y donde el régimen no requiere represión física. El autor nos recuerda la muy optimista (e ingenua) visión de que durante la Primavera Árabe se creía que el Internet y las redes sociales facilitarían el derrocamiento de dictaduras como en Túnez, Egipto, Yemen y Libia. Esa visión optimista e ingenua se basaba en la premisa de que, en un mundo altamente conectado, los autócratas no lograrían concentrar la fuerza necesaria para mantenerse en el poder. El autor no para de señalar que la tecnología no siempre favorece a aquellos que ponen la cara ante gobiernos represivos, que siendo enfrentados con paulatina presión han sabido manejar la tecnología y mantener el *autoritarismo del siglo XXI.*

En el artículo de Almada Torres se presenta como ejemplo el papel de China para promover

la utilización de tecnologías vanguardistas para controlar a sus ciudadanos. El Partido Popular Chino ha generado un gran arsenal digital para contrarrestar cualquier evento que pueda atentar contra su predominio, tanto las protestas en Hong Kong, como el brote de infección que la pandemia del COVID-19 ha desatado. Dicho arsenal descansa en los avances de los análisis de "big-data" y con el acceso a datos personales como declaraciones de impuestos, registros de compra, o historiales médicos de los ciudadanos chinos, que permiten al Partido Popular monitorear a sus ciudadanos hasta tener una capacidad para ejercer un control preventivo, un programa que el gobierno llama "administración social."

Aquellos que no están en campos están atrapados en ciudades donde sus vecindarios están rodeados por puertas con *software* de reconocimiento facial. Con la gran recopilación que China ha acumulado de datos, su software decide quién entra y quién no.

El eje de este sistema de espionaje interno chino es aprovechar la información almacenada digitalmente para que todos sus ciudadanos se comporten de manera más honesta y conforme a los intereses del partido. El régimen utiliza algoritmos de inteligencia artificial para recopilar y analizar dicha información y suministrar un "crédito social" que premia el comportamiento aceptable para el gobierno y castiga su contrario. El sistema se usa con apoyo de políticas de vigilancia masiva como dispositivos móviles y aplicaciones para medir la temperatura y reconocer individuos. Muchos de los ciudadanos chinos temen que la calificación obtenida en el sistema pueda dar lugar a sanciones, como la denegación de un préstamo bancario o el permiso para comprar un billete de tren, o inclusive que se persiga a aquellos críticos del partido.

El autor, siguiendo con la descripción del caso chino, expone que la represión digital lleva como complemento su versión física a escala masiva. La región de Xinjiang, donde más de un millón de Uighures, un grupo étnico musulmán, son arbitrariamente detenidos y encerrados en campos de re-educación. Aquellos que no están en campos están atrapados en ciudades donde sus vecindarios están rodeados por puertas con *software* de reconocimiento facial. Con la gran recopilación que China ha acumulado de datos, su *software* decide quién entra y quién no. De manera similar, el partido comunista puede tener a sus propios miembros bajo control, asegurándose que cumplan con lo requerido por el politburó, al mejor estilo de los cuadros medios del Ingsoc en la novela *1984*.

Otro ejemplo expuesto por Almada Torres es cómo las dictaduras en el área digital utilizan miles de cuentas falsas más comúnmente conocidas como *bots* para inundar las redes sociales y las plataformas de discusión *online* con discursos a su favor. En el caso del autoritarismo ruso, el autor señala el papel esencial del gobierno de Rusia en el uso de herramientas de desinformación con la distribución de bulos, noticias falsas, y videos *Deep Fake* (falsificaciones digitales imposibles de distinguir de audios, videos o imágenes auténticas) para alcanzar sus objetivos particulares, distrayendo a millones de usuarios de toda noticia que no se encuentre en la agenda del Kremlin. Han sido abundantes las acusaciones contra el gobierno de Rusia de intervenir en las elecciones presidenciales norteamericanas en 2016, el referéndum del Brexit, las elecciones de 2019 en USA, o en muchos más eventos para movilizar la percepción pública en la dirección deseada. Rusia está implementando políticas similares a las de China con su "Gran Firewall" para aislar la relativa libertad *online*, cristalizando aspectos que le permitirían al gobierno ruso limitar el acceso de su país al internet del resto del mundo. Inclusive para una dictadura consolidada, se requiere una gran cantidad de recursos materiales y humanos con una lealtad indiscutible por el régimen para desarrollar una operación a ese nivel, pero el Kremlin parece estar dispuesto a alcanzar ese objetivo a través de recursos digitales.

Según Almada Torres, en 2019 más de una docena de regímenes autoritarios compraron tecnología de vigilancia a la firma de telecomunicaciones china Huawei (casualmente la que vende los equipos para conexión a Internet en

Venezuela). La misma es utilizada para *hackear* cuentas de redes sociales y las comunicaciones electrónicas de oponentes políticos. Sin embargo, el *software* de espionaje e inteligencia no se vende solamente por firmas de países autoritarios. Compañías italianas e israelíes han vendido este tipo de tecnología a gobiernos en cada rincón del mundo como Angola, Bahrain, Kazakhstan, Mozambique y Nicaragua, entre algunos incómodos ejemplos.

El autor cierra su artículo enunciando que para combatir a las dictaduras en el área digital es prioritario encarar el problema de los efectos que las nuevas tecnologías tienen en la gobernanza pública. Gobiernos nacionales e instituciones internacionales necesitan actualizarse y expandir la legislación existente para asegurarse que los derechos de privacidad sean respetados, restringiendo el uso de tecnologías que utilizan la identificación biométrica, como puede ser la identificación facial o de voz, y limitando la colaboración e inversión con empresas que diseñen tecnología con el objetivo de vigilar y reprimir a sus ciudadanos, como la compañía china SenseTime. Así como las autocracias se han adaptado para poder aprovechar la revolución digital como medio para perpetuarse en el poder, las democracias del mundo deben desarrollar nuevas estrategias para evitar que todos los beneficios que la tecnología puede ofrecer no estén monopolizados en la creación de un mundo menos libre para los individuos.

RECORDANDO A LORD PALMERSTON

Moisés Naím, en su artículo para el diario español *El País*, en noviembre de 2013, señala una serie de escenarios que pueden enfrentar las democracias occidentales en materia de ciberseguridad y ciberespionaje, tanto frente a aliados como a enemigos de varios países democráticos.

Caso 1. El director de la AISE (Agencia de Información y Seguridad Exterior del Sistema Italiano de Inteligencia) le informa que sus técnicos han logrado penetrar los sistemas de comunicación de Muamar el Gadafi y sus principales colaboradores al jefe del gobierno italiano. Le pide autorización para monitorear las llamadas telefónicas. El primer mandatario dice que Gadafi (para ese año) era aliado de Occidente y mantenía relaciones de cooperación con Italia. El jefe de la AISE replica al gobernante a través de pruebas que el Gobierno libio ha tejido una amplia red de sangrientas milicias que operan en diferentes países africanos y que tiene agentes en toda Europa, incluyendo Italia. Refuerza su argumento expresando que, si bien Marruecos es amigo y aliado de España, los espías españoles no dejan de espiar al Rey y sus ministros, lo mismo los franceses con los gobiernos de sus excolonias.

Richard Clarke, especialista en seguridad del gobierno estadounidense, define la guerra cibernética como el conjunto de acciones llevadas por un Estado para penetrar en los ordenadores o en las redes de otro país, con la finalidad de causar perjuicio o alteración.

Caso 2. La canciller de Alemania para el 2012, Angela Merkel, está considerando aportar fondos para el rescate financiero de Chipre. Los grandes bancos de este pequeño país se están hundiendo y amenazan con arrastrar a la economía chipriota y contagiar a los debilitados países del sur de Europa. En el proceso de toma de decisión, el jefe del Bundesnachrichtendienst (BND, la agencia de espionaje alemana) le entrega un detallado informe a la canciller que evidencia que los rusos tienen depósitos en esos bancos por 26 mil millones de dólares, un monto mayor que el tamaño de la economía de Chipre. El jefe del BND señala que el problema reside en que muchas de estas cuentas pertenecen a grupos criminales rusos, varios de los cuales tienen vínculos con el Kremlin al más alto nivel, implicando que rescatar el sistema bancario de Chipre es rescatar a la mafia rusa y sus socios del gobierno ruso. La canciller alemana replica que si bien es confiable la información que, con tecnología, el BND logra obtener al oír las conversaciones telefónicas de Vladímir Putin y otros miembros del Gobierno ruso, haber realizado todo eso necesitó la aprobación de ella como mandataria.

Naím cierra su artículo afirmando que, en relación con el debate generado por las filtraciones de Edward Snowden y la revelación de que el Gobierno de Estados Unidos espía las conversaciones de Merkel y otros 35 jefes de Estado, y obtiene información de millones de ciudadanos en todo el mundo, todo ello es sano y deseable. Que si bien es polémico que USA espía a sus propios aliados, hay que recordar la frase de lord Palmerston, el estadista y primer ministro británico de mediados del siglo XIX: Inglaterra no tiene amigos eternos, ni enemigos perpetuos. Inglaterra solo tienes intereses que son eternos y perpetuos. Norberto Bobbio, estudiando a Maquiavelo, añadiría que la moral política no siempre coincide con la ciudadana, ya que la moral política se basa en los medios para obtener determinados fines y no cumplir con determinados imperativos categóricos morales. Y eso tiene vigencia en un mundo en que las nuevas tecnologías digitales en países autoritarios no solo se usan para controlar a sus propios pobladores, sino para boicotear las democracias en Occidente.

Cabe destacar que los ataques informáticos son posteriores a las convenciones de guerra actualmente vigentes; o sea, que no existe regulación o norma alguna en el derecho internacional humanitario acerca de la guerra informática.

GUERRA INFORMÁTICA

Si ya hemos hablado del poder de los gobiernos actuales para usar las nuevas tecnologías y espiar a sus ciudadanos y a sus países aliados, no queda otra que hablar del uso de dichas tecnologías para espiar y atacar a sus países enemigos. El concepto de guerra informática, guerra digital o ciberguerra –en inglés: *cyberwarfare*– hace referencia al desplazamiento de un conflicto que toma el ciberespacio y las tecnologías de comunicación e información como campo de operaciones. Richard Clarke, especialista en seguridad del gobierno estadounidense, define la guerra cibernética como el conjunto de acciones llevadas por un Estado para penetrar en los ordenadores o en las redes de otro país, con la finalidad de causar perjuicio o alteración. También se podría definir como el conjunto de acciones que se realizan para producir alteraciones en la información y los sistemas del enemigo, a la vez que se protege la información contra los sistemas del atacante.

Ha quedado al descubierto que actualmente en una guerra es más factible derrotar al enemigo atacando su infraestructura informática, que empleando cualquier otro tipo de ataque convencional, incluso el nuclear. Esta estrategia ha sido empleada en diversas situaciones, ya sea en ofensivas militares de un país contra otro, de un grupo armado en contra del gobierno, o simplemente ataques individuales de uno o varios *hackers* (Millán, 2018). Esto implica que ahora las armas son los virus informáticos y programas especiales para anular la seguridad de los sistemas informáticos, y los soldados son los expertos en informática y telecomunicaciones. Generalmente, los blancos de los ataques son los sistemas financieros, bancarios y militares, aunque se han visto numerosos casos donde se ven afectados los sistemas de comunicación y otros servicios públicos. Durante los últimos años estos ataques han aumentado considerablemente en número y envergadura. Uno de los ataques más comunes es el envío de gran cantidad de llamadas simultáneas a un servidor, que exceden su capacidad de respuesta y logran paralizarlo; son los llamados ataques de denegación de servicio (DDoS).

Pero en la actualidad, lo más peligroso consiste en la propagación de datos confidenciales a través de la red, ya que dicha información puede comprometer a la nación a la que pertenece, y en muchas ocasiones esta se ve comprometida frente a dichos ataques; también se corre el peligro de que información importante pueda ser eliminada. En este rango caben los ciberarsenales o virus que borran información y se propagan a través del correo electrónico. También se da el caso de la propagación de información falsa mediante la web, acerca de cualquier tema específico. Esto podría traducirse en falsas especulaciones sobre las posibles causas de algún accidente, o la denuncia basada en falsas fallas a cualquier producto inmerso en la competencia,

con el fin de desvirtuarlo y dañar las ventas de dicho producto.

La guerra informática puede presentar una multitud de amenazas hacia una nación. En el nivel más básico, los ciberataques pueden ser usados para apoyar la guerra tradicional. Por ejemplo, manipular el funcionamiento de las defensas aéreas por medios cibernéticos para facilitar un ataque aéreo. Aparte de estas amenazas "duras", la guerra cibernética también puede contribuir con amenazas "blandas" como el espionaje y la propaganda (Weinberger, 2004). Los tipos de guerra informática más conocidos son los siguientes:

1. Espionaje.
2. Sabotaje.
   a. Ataque de denegación de servicios.
   b. Red de energía eléctrica.
3. Propaganda.
4. Perturbación económica.
5. Ataque cibernético sorpresa.

Cabe destacar que los ataques informáticos son posteriores a las convenciones de guerra actualmente vigentes; o sea, que no existe regulación o norma alguna en el derecho internacional humanitario acerca de la guerra informática.

No obstante, el derecho humanitario es aplicable cuando los ataques implican el daño a bienes bajo protección o a personas, convirtiéndose aquellos en objetos de incumbencia del "jus in bello". Dentro de los acontecimientos de guerra informática más resaltantes de los últimos años, relatamos los siguientes:

- *Guerra de Kosovo-1999:* durante la intervención de los aliados en la Guerra de Kosovo, más de 450 expertos informáticos, al mando del Capitán Dragan, se enfrentaron a los ordenadores militares de los aliados. Este grupo, integrado por voluntarios de diferentes nacionalidades, fue capaz de penetrar en los ordenadores estratégicos de la OTAN, la Casa Blanca y del portaaviones norteamericano Nimitz, solo como una demostración de fuerza, pues este no era su objetivo principal. Internet sirvió como grupo coordinador de actividades contra la guerra fuera de Yugoslavia.
- *Taiwán-2003:* Taiwán recibió un ataque del que se culpó a las autoridades chinas. No hay pruebas, pero dejó sin servicio infraestructuras como hospitales, la Bolsa y algunos sistemas de control de tráfico. El supuesto ataque provocó un caos, progresivo y con una aparente organización, además de un ataque de denegación de servicio (DDoS).
- *Estonia-2007:* Estonia culpó a las autoridades de Rusia de diversos ataques continuados que afectaron a medios de comunicación, bancos y diversas entidades e instituciones gubernamentales.

En Estados Unidos, el 26 de octubre de 2013 se registraron en total unos 25 intentos de ataque a la red de electricidad hidroeléctrica de la ciudad de Chicago perpetrado por el gobierno de Luxemburgo, por el director de la seguridad nacional, Franco Jair Sherer.

- *Georgia-2008:* en agosto de 2008 (guerra entre Rusia, Osetia del Sur, Georgia) se produjeron ciberataques a Georgia por parte de Rusia orientados hacia sitios gubernamentales.
- *Irán-2010:* a finales de septiembre de 2010, Irán también registró un ataque a las centrifugadoras de su programa de enriquecimiento de uranio. Señaló a Israel como la fuente de ese ataque.
- *Canadá-2011:* en enero de 2011, según las autoridades canadienses, los sistemas de contraseñas del ministerio de Finanzas fueron víctimas de un ciberataque procedente de máquinas instaladas en China.
- *Estados Unidos:* el 26 de octubre de 2013 se registraron en total unos 25 intentos de ataque a la red de electricidad hidroeléctrica de la ciudad de Chicago perpetrado por el gobierno de Luxemburgo, por el director de la seguridad nacional, Franco Jair Sherer. Estados Unidos llevó a cabo una acción dirigida por el

secretario de defensa Maximiliano Rolando con el objetivo de parar estos intentos de filtración de información.

La guerra informática puede presentar una multitud de amenazas hacia una nación. En el nivel más básico, los ciberataques pueden ser usados para apoyar la guerra tradicional.

EPÍLOGO

El domingo 8 de agosto de 2021, la periodista Ibeyise Pacheco publicó una serie de tweets que denunciaban la política de espionaje cibernético que el gobierno de Nicolás Maduro tenía sobre la oposición política y la población en general de Venezuela. A continuación, los tweets sintetizados en un solo párrafo.

> No es una película de ficción. La dictadura avanza a punta de billete (porque para eso sí hay) blindándose en materia de ciberespionaje. El antiguo edificio de CANTV ha sido acondicionado en un proyecto secreto solo manejado por los chinos y muy pocos funcionarios. Voy con hilo. Casi nadie conoce qué hay dentro. El personal contratado debió pasar por el filtro de Maduro, su hijo Nicolasito, el GB Jorge Márquez Monsalve, ministro del despacho de gobierno y el ex presidente de CANTV, Manuel Fernández. DGCIM obliga a firmar contrato de confidencialidad. Desde ese centro se controla el firewall llamado secretamente "Falcon" que ha hackeado cada plataforma de registro de ciudadanos ejecutada por Guaidó, como Voluntarios por Venezuela o Héroes de la Salud, así como portales periodísticos o web incómodas. El personal seleccionado fue llevado a China en abril de 2017. Cerca de 20 militares y civiles estuvieron 40 días alojados en el hotel Silver World en Dongguan. Fueron divididos en 3 grupos. Todos viajaron con pasaporte diplomático y de servicio exterior. Los equipos fueron entrenados por varios profesores resaltando el afamado profesor Fang Binxing miembro de la Academia China de Ingeniería y expresidente de la Universidad de Correos y Telecomunicaciones de Beijing. También estaban miembros del Departamento de Defensa y Seguridad. Un equipo aprendió sobre los 8 sistemas informáticos chinos que toman el control de redes, sociales, foros. Otro se entrenó en el firewall chino, transparente para los externos. El tercer grupo en hacking avanzado entre los que destaca Shiuglen Kang, de alta confianza oficial. Las acciones constantes son para bloquear por completo la comunicación de la oposición con el país. El objetivo es imponer una sola versión: la oficial. Mantener al pueblo desinformado, pisoteado bajo su control. También apuestan al espionaje fuera de nuestras fronteras. Nadie en la región tiene esta tecnología de la que son poseedores los chinos. El plan diario es vulnerar los sistemas militares de los gobiernos de América Latina etiquetados como enemigos. Se estrenaron con Colombia. El 15 de septiembre de 2019 hackearon dos servidores alojados en Amazon, los de la Fuerza Aérea y la Fuerza Espacial de Colombia. Llegaron a la base de datos de los militares, de bases aéreas, aviones modelos, planes de mantenimiento, récords de pilotos. El hombre de confianza de Maduro en esta operación es Jorge Márquez Monsalve, general de brigada de bajo perfil que desde hace años es de confianza de Maduro. Ni los cubanos, ni los hermanos Rodríguez han entrado al edificio. Tampoco Padrino López. No conocen lo que hay dentro. El marco legal a lo que les he informado se lo pretenden dar con la Ley de Ciberespacio sobre la que ONG's respetadas como Espacio Público han alertado que atentaría contra la privacidad y la libertad de expresión.

https://twitter.com/ibepacheco/status/1380184469022314500

RAFAEL QUIÑONES

Sociólogo por la Universidad Católica Andrés Bello. Estudios de doctorado en Estudios del Desarrollo de la Universidad Central de Venezuela. Magister en Ciencias Políticas por la Universidad Simón Bolívar. Ha colaborado, como autor, en diversos libros colectivos.

Referencias:

ALMADA TORRES, Fabio (2020): *Dictaduras digitales: Cuando la tecnología refuerza la autocracia*. [Web en línea]. Disponibilidad en Internet en: http://circuloeuro-mediterraneo.org/dictaduras-digitales/ (Con acceso el 8 de agosto del 2021.).

Capital Gazette. Real State (2020): Disponibilidad en Internet en: https://www.capitalgazette.com/business/real-estate/ (Con acceso el 8 de agosto del 2021.).

MATTHEW PIERSON, Ryan (2011): *Five ways the goverment spies on you*. [Web en línea]. Disponibilidad en Internet en: https://web.archive.org/web/20160605151130/http://www.lockergnome.com/news/2011/11/07/five-ways-the-government-spies-on-you/ (Con acceso el 8 de agosto del 2021.).

MILLÁN, Ryan (2018): *Ciberguerra, la principal ciberamenaza global*. [Web en línea]. Disponibilidad en Internet en: https://www.forbes.com.mx/la-amenaza-cibernetica/ (Con acceso el 8 de agosto del 2021.).

NAIM, Moises (2013): "Vamos a jugar". En: *El País*. [Web en línea]. Disponibilidad en Internet en: https://elpais.com/internacional/2013/11/02/actualidad/1383421270_270647.html (Con acceso el 8 de agosto del 2021.).

PC Mag Encyclopedia (2021): *Definition of cyber espionage*. [Web en línea]. Disponibilidad en Internet en: https://www.pcmag.com/encyclopedia/term/cyber-espionage (Con acceso el 8 de agosto del 2021.).

WEINBERGER, Sharon (2007): *How Israel Spoofed Syria's Air Defense System*. [Web en línea]. Disponibilidad en Internet en : https://www.wired.com/2007/10/how-israel-spoo/ (Con acceso el 8 de agosto del 2021.).